The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE ISSUED:
01/17/2017

SUBJECT:
Oracle Quarterly Critical Patches Issued January 17, 2017

OVERVIEW:
Multiple vulnerabilities have been discovered in Oracle products, which could allow for remote code execution.

SYSTEMS AFFECTED:
- Oracle Database Server, version(s) 11.2.0.4, 12.1.0.2
- Oracle Secure Backup, version(s) prior to 12.1.0.2.0, prior to 12.1.0.3
- Spatial, version(s) prior to 1.2
- Oracle Fusion Middleware, version(s) 11.1.1.7, 11.1.1.9, 11.1.2.3, 11.1.2.4, 12.1.3.0, 12.2.1.0, 12.2.1.1
- Oracle GlassFish Server, version(s) 2.1.1, 3.0.1, 3.1.2
- Oracle JDeveloper, version(s) 11.1.1.7.0, 11.1.1.9.0, 11.1.2.4.0, 12.1.3.0.0, 12.2.1.0.0, 12.2.1.1.0, 12.2.1.2.0
- Oracle Outside In Technology, version(s) 8.5.2, 8.5.3
- Oracle Tuxedo, version(s) 12.1.1
- Oracle WebLogic Server, version(s) 10.3.6.0, 12.1.3.0, 12.2.1.0, 12.2.1.1
- Application Testing Suite, version(s) 12.4.0.2, 12.5.0.2, 12.5.0.3
- Enterprise Manager Base Platform, version(s) 12.1.0.5, 13.1, 13.2
- Enterprise Manager Ops Center, version(s) 12.1.4, 12.2.2, 12.3.2
- Oracle E-Business Suite, version(s) 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6
- Oracle Transportation Management, version(s) 6.1, 6.2
- PeolpeSoft Enterprise HCM ePerformance, version(s) 9.2
- PeopleSoft Enterprise PeopleTools, version(s) 8.54, 8.55
- JD Edwards EnterpriseOne Tools, version(s) 9.2.1.1
- Siebel Applications, version(s) 16.1
- Oracle Commerce Platform, version(s) 10.0.3.5, 10.2.0.5, 11.2.0.2
- Oracle Fusion Applications, version(s) 11.1.2 through 11.1.9
- Oracle Communications Indexing and Search Service, version(s) prior to 1.0.5.28.0
- Oracle Communications Network Charging and Control, version(s) 4.4.1.5, 5.0.0.1, 5.0.0.2, 5.0.1.0, 5.0.2.0
- Oracle Communications Network Intelligence, version(s) 7.3.0.0
- Oracle FLEXCUBE Core Banking, version(s) 5.1.0, 5.2.0, 11.5.0

- Oracle FLEXCUBE Direct Banking, version(s) 12.0.0, 12.0.1, 12.0.2, 12.0.3
- Oracle FLEXCUBE Enterprise Limits and Collateral Management, version(s) 12.0.0, 12.0.2
- Oracle FLEXCUBE Investor Servicing, version(s) 12.0.1, 12.0.2, 12.0.4, 12.1.0, 12.3.0
- Oracle FLEXCUBE Private Banking, version(s) 2.0.1, 2.2.0, 12.0.1
- Oracle FLEXCUBE Universal Banking, version(s) 11.3.0, 11.4.0, 12.0.0, 12.0.1, 12.0.2, 12.0.3, 12.1.0, 12.2.0
- MICROS Lucas, version(s) 2.9.1, 2.9.2, 2.9.3, 2.9.4, 2.9.5
- Oracle Retail Allocation, version(s) 12.0, 13.0, 13.1, 13.2, 13.3, 14.0, 14.1
- Oracle Retail Assortment Planning, version(s) 14.1, 15.0
- Oracle Retail Order Broker, version(s) 4.1, 5.1, 5.2, 15.0, 16.0
- Oracle Retail Predictive Application Server, version(s) 13.1, 13.2, 13.3, 13.4, 14.0, 14.1, 15.0
- Oracle Retail Price Management, version(s) 13.1, 13.2, 14.0, 14.1
- Primavera P6 Enterprise Project Portfolio Management, version(s) 8.2, 8.3, 8.4, 15.1, 15.2, 16.1, 16.2, 17.1, 16.2. 17.1
- Oracle Java SE, version(s) 6u131, 7u121, 8u112
- Oracle Java SE Embedded, version(s) 8u111
- Oracle JRockit, version(s) R28.3.12
- Oracle VM Server for Sparc, version(s) 3.2, 3.4
- Solaris, version(s) 11.3
- Oracle VM VirtualBox, version(s) prior to 5.0.32, prior to 5.1.14
- MySQL Cluster, vers

ion(s) 7.2.26 and prior, 7.3.14 and prior, 7.4.12 and prior
- MySQL Enterprise Monitor, version(s) 3.1.3.7856 and prior, 3.1.4.7895 and prior, 3.1.5.7958 and prior, 3.2.1.1049 and prior, 3.2.4.1102 and prior, 3.3.0.1098 and prior
- MySQL Server, version(s) 5.5.53 and prior, 5.6.34 and prior, 5.7.16 and prior

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: High

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Oracle to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Oracle:
http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html